digicert

Company Registration No.: 1998/003036/07

PAIA INFORMATION MANUAL

OF

DIGICERT SOUTH AFRICA PROPRIETARY LIMITED (DIGICERT)

("PAIA MANUAL")

Prepared in accordance with

Section 51 of the Promotion of Access to Information Act, No. 2 of 2000 (as amended) ("the Act")

and

the Protection of Personal Information Act, No. 4 of 2013.

Initials MJ Initials EP

digicert

TABLE OF CONTENTS

Initials MJ Initials EP

1. INTRODUCTION TO DIGICERT

DigiCert is the leading provider of digital trust with its main function as a digital certificate authority. As the world's leading provider of scalable TLS/ SSL, IoT and PKI solutions for identity and encryption, DigiCert company is recognized for its enterprise- grade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions. DigiCert South Africa Proprietary Limited is a member of the DigiCert Group headquartered in the United States.

2. INFORMATION REQUIRED UNDER SECTION 51(1)(a) OF THE ACT

Head of Private Body/Information Officer	Michael Johnson, Director A. Eric Porter, Director
Postal Address	Floors 3, 4, & 5 Gateway Building Century Blvd & Century Way 1 Century City Cape Town, Western Cape 7441 South Africa
Street Address	Floors 3, 4, & 5 Gateway Building Century Blvd & Century Way 1 Century City Cape Town, Western Cape 7441 South Africa
Telephone Number	+1-800-896-7973
Fax Number	n/a
Email	support@digicert.com
Deputy Information Officer (to handle requests)	Aaron Olsen
Email address of Deputy Information Officer	privacy@digicert.com

3. DESCRIPTION OF GUIDE REFERRED TO IN SECTION 10

3.1 The ACT grants a requester access to records of a private body, if the record is required fo the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

3.2 Requests in terms of the ACT shall be made in accordance with the prescribed procedures at the rates provided. The forms and tariff are dealt with in paragraphs 6 and 7 of the Act

3.3 Requesters are referred to the Guide in terms of Section 10 which has been compiled by t South African Human Rights Commission, which will contain information for the purposes exercising Constitutional Rights. The Guide is available from the SAHRC.

The contact details of the Commission are:

Postal Address:	Private Bag 2700, Houghton, 2041
Telephone Number:	+27-11-877 3600
Fax Number:	+27-11-403 0625
Website:	www.sahrc.org.za

4. APPLICABLE LEGISLATION

Ref	Act
No. 75 of 1997	Basic Conditions of Employment Act
No. 53 of 2003	Broad-Based Black Economic Empowerment Act
No. 71 of 1991	Business Act
No. 71 of 2008	Companies Act
No. 130 of 1993	Compensation of Occupation Injuries and Diseases Act
No. 89 of 1998	Competition Act
No. 98 of 1978	Copyright Act
No. 19 of 2020	Cybercrimes Act
No. 36 of 2005	Electronic Communications Act
No. 25 of 2002	Electronic Communications and Transactions Act
No. 55 of 1998	Employment Equity Act
No. 68 of 1997	Identification Act
No. 95 of 1967	Income Tax Act
No. 38 of 1997	Intellectual Property Laws Amendment
No. 66 of 1995	Labour Relations Act
No. 85 of 1993	Occupational Health and Safety Act

Initials MJ Initials EP

No. 2 of 2000	Promotion of Access of Information Act
No. 4 of 2013	Protection of Personal Information Act
No. 194 of 1993	Trademarks Act
No. 63 of 2001	Unemployment Contributions Act
No. 30 of 1996	Unemployment Insurance Act
No. 89 of 1991	Value Added Tax Act

The accessibility of documents and records may be subject to the grounds of refusal as set out in this PAIA Manual.

5. RECORDS AUTOMATICALLY AVAILABLE

No notice has been submitted by DigiCert to the Minister of Justice and Constitutional Development regarding the categories of records, which are available without a person having to request access in terms of Section 52(2) of PAIA. However, the information on the website of the business and an end user's account platform is automatically available without having to request access in terms of PAIA.

6. SUBJECTS AND CATEGORIES OF RECORDS HELD BY DIGICERT

General information about DigiCert can be accessed via the internet at www.digicert.com, which is available to all individuals who have access to the internet.

The subjects of which the company holds various records and the categories on each subject in terms of Section 51(1)(e) are as listed below. Please note that a requester is not automatically allowed access to these records and that access to such records may be refused in accordance with Sections 62 through 69 of the Act.

a. Companies Act Records
    a. Documents of Incorporation
    b. Memorandum of Incorporation
    c. Minutes of meeting of the Board of Directors
    d. Resolutions of the Board of Directors
    e. Records relating to the appointment of corporate officers

b. Financial Records
    a. Accounting records
    b. Annual financial reports
    c. Annual financial statements

Initials MJ Initials EP

d. Banking details and bank accounts
e. Debtors/Creditors statements and invoices
f. Policies and procedures
g. Tax returns

c. Income Tax Records
   a. PAYE Records
   b. Documents issued to employees for income tax purposes
   c. Records of payments made to SARS on behalf of employees
   d. All other statutory compliance records, including:
      i. VAT
      ii. UIF
      iii. Workmen's Compensation

d. Personnel Documents and Records
   a. Accident books and records
   b. Address lists
   c. Disciplinary code and records
   d. Employee benefits arrangements rules and records
   e. Employment contracts
   f. Forms and applications
   g. Grievance procedures
   h. Leave records
   i. Medical aid records
   j. Payroll reports/wage register
   k. Salary records
   l. Standard letters and notices
   m. Training manuals
   n. Training records

e. Procurement Department
   a. Standard terms and conditions for supply of services and products
   b. Contractor, client, and supplier agreements
   c. Lists of suppliers, products, services, and distribution
   d. Policies and procedures

f. Sales Department
   a. Customer details
   b. Information and records provided by a third party
   c. Policies and procedures

Initials MJ Initials EP

g. Marketing Department
   a. Advertising and promotional material
   b. Policies and procedures

h. Compliance and Audit Department
   a. Audit reports
   b. Policies and procedures
   c. Risk management frameworks
   d. Risk management plans

i. IT Department
   a. Disaster recovery plans
   b. Information technology systems and user manuals
   c. Policies and procedures
   d. System documentation and manuals

7. PURPOSE OF PROCESSING OF PERSONAL INFORMATION

The transfer is made for the following illustrative but not exhaustive purposes:

- Facilitating staff and business administration;
- Making group-wide strategic business decisions, particularly with respect to staffing, succession planning, renumeration and personnel deployment and assignment;
- Reference and risk mitigation;
- Managing vendor, partner, reseller and other third-party relationships consistently throughout the DigiCert Group;
- Reviewing personal information provided by customers to facilitate the issuance of digital certificates and to provide related services to our customers; and,
- Communicating with our customers regarding DigiCert Group services and products.

Additional details can be found in our Global Public Privacy Notice available at www.digicert.com.

8. DATA SUBJECTS CATEGORIES AND THEIR PERSONAL INFORMATION

Current, past and prospective personnel of DigiCert Group.

The personal information of DigiCert Group personnel generated in the normal course of employment and staff and business administration.

Initials MJ Initials EP

Current, past and prospective agents and employees of DigiCert Group customers, partners, resellers, vendors and other third parties who provide personal information to DigiCert Group in order for DigiCert Group to provide services or to work with said entities.

Personal information of DigiCert Group customers, partners, resellers, vendors and other third parties collected through performing services for customers and in working with other third parties in the regular course of business or as otherwise collected through such individuals' use and enjoyment of DigiCert Group equipment, networks, and systems.

9. PLANNED RECIPIENTS OF PERSONAL INFORMATION

The personal information transferred may be disclosed only to the following recipients or categories of recipients for as long as necessary to effectuate the purpose of processing or as may be otherwise required by law:

- Member entities of DigiCert Group
- Third-party service providers (such as staff and benefits administrators or IT systems and hosting services providers);
- Legal counsel or other advisors;
- In the case of sale, change or control or transfer of all or part of the assets of the DigiCert Group (or any of its component entities) the personal information may be disclosed to a purchaser or investor (or a potential purchaser or investor) and their advisors; and,
- In line with normal practice, routine personnel contact information and details may be provided to DigiCert Group customers or potential customers in the ordinary course or carrying out work (this may include for example, providing personnel's business email to potential customer to enable them to contact him or her).

10. TRANS-BORDER FLOWS OF PERSONAL INFORMATION

Personal information is transferred to the United States, European Economic Area, Switzerland, India, Japan, and Australia.

11. SECURITY MEASURES TO PROTECT PERSONAL INFORMATION

DigiCert's technical and organizational controls align with industry standards and business needs to achieve appropriate levels of privacy and security. The following list of controls outlines DigiCert's minimum baseline of standard practices to safeguard data.

- Policy and Document Management – DigiCert keeps, reviews annually at a minimum, and tests an Information Security Policy, Business Continuity Plan, Disaster Recovery Plan, and Incident Response Process. DigiCert maintains and updates as necessary an intra-group data sharing agreement and appropriate vendor Data Processing Agreements. In addition to publicly posted privacy notices applicable to DigiCert products and services, DigiCert also maintains and

reviews/updates on an annual basis an internal Framework Privacy Policy, governing privacy standards and processes applicable to DigiCert.

- Network Security Controls – DigiCert's System Administrators ensure that publicly accessible information system components (e.g., public web servers) reside on separate sub-networks with separate physical network interfaces. DigiCert's System Administrators also ensure that controlled interfaces protecting the network perimeter filter certain types of packets to protect devices on DigiCert's internal network. Firewalls and boundary control devices are configured to allow access only to what is necessary to perform DigiCert's operations.
- Database Security Controls – All access (via system or directly by personnel) to DigiCert databases is logged and monitored for unauthorized changes. Data is encrypted in databases using an industry-recommended cipher, and direct access is limited to roles as specified by DigiCert's Information Security Policy and Certification Practices Statement.
- Access Controls and Authentication – All user interactions with DigiCert systems are traceable to the individual performing such actions and all users must be positively identified prior to being able to interact with DigiCert systems. DigiCert personnel must first authenticate themselves to DigiCert systems before they are allowed access to any components of the system necessary to perform their trusted roles and roles are defined by DigiCert's Certification Practices Statement and Information Security Policy. User accounts and other types of access to DigiCert computer systems must be approved in accordance with the User Access Policy. Both physical and logical controls, as outlined in applicable policies, to authorized individuals are reviewed periodically and, at minimum, yearly.
- Personnel Controls – All DigiCert employees and other workers with access to DigiCert data and/or systems are subject to confidentiality agreements and are required to pass background checks and have specific, role-based training. DigiCert maintains and enforces policies and procedures for trusted roles, identification and authentication for each role, sanctions for unauthorized actions, separation of duties, employee badging, and immediate removal of system access for terminated employees/workers.
- Physical Security Controls – Access to every office, computer room, and work area containing sensitive information is physically restricted. All office doors have a lock, and all entrance doors to DigiCert facilities are always locked. These doors are accessible by an Access Card or other access control device, which is issued upon confirmation of a clean background check. DigiCert data centers, cages, and offices are monitored by CCTV. The secured cage requires biometric and dual custodian personnel for access. All access is logged.
- Vulnerability Management/Patching – Monthly scans are performed on all DigiCert assets using vulnerability detection tools. Systems requiring remediation are required to be patched within timelines defined by Global Security Operations. Timelines are based on the assigned Common Vulnerability Scoring System (CVSS) score. Critical and high vulnerabilities are patched within 72 hours or have a plan of action created, medium vulnerabilities are patched or have a plan of action created within 30 days, and low/information vulnerabilities are patched at DigiCert's discretion.
- Comprehensive Internal Assessment – DigiCert performs an annual comprehensive risk assessment to identify all of the reasonably foreseeable internal and external threats to security, privacy, confidentiality, and integrity.

Initials MJ Initials EP

- Penetration Assessment/External Assessment – At least one third-party penetration assessment is conducted each year. DigiCert typically performs multiple penetration tests per year on code, infrastructure, and systems as well as completing red team assessments.
- Training and Awareness – All employees and other workers are required to undergo annual privacy, security, and compliance training. Employees or others handling personally identifiable information and sensitive information receive additional training. All workers with access to DigiCert systems and/or data are required to adhere to policies and procedures for proper data handling, such as DigiCert's Information Security Policy, Code of Conduct, and Acceptable Use Policy.
- Third-Party Access Controls – DigiCert's contracts with third parties who may access DigiCert systems or data adequately address security and privacy requirements. These third parties are also subject to a privacy and security impact assessment and risks are mitigated prior to access.
- Data Protection in Storage and Transmission – All data stored in DigiCert systems is encrypted using an industry-recommended cipher. Likewise, all data transmitted within DigiCert systems worldwide is encrypted in transit using an industry-recommended cipher.
- Storage, Retention, and Deletion – Information stored physically or electronically have the appropriate technical controls determined by the level of data classification. Information is deleted in accordance with our CP/CPS and applicable privacy notices.

12. DETAIL ON HOW TO MAKE A REQUEST FOR ACCESS

Use the prescribed form, available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za, and made available at the end of this Manual.

- Address your request to the Deputy Information Officer.
- Provide sufficient details to enable the COMPANY to identify:
  - The record(s) requested;
  - The requester (and if an agent is lodging the request, proof of capacity);
  - The form of access required;
  - The postal address or fax number of the requester in the Republic;
  - If the requester wishes to be informed of the decision in any manner (in addition to written) the manner and particulars thereof; and,
  - The right which the requester is seeking to exercise or protect with an explanation of the reason the record is required to exercise or protect the right.

Payment of fees as may be required. A requester who seeks access to a record containing personal information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee:

- The Deputy Information Officer will by written notice require each requester (other than a personal requester) to pay the prescribed request fee (if any) before further processing any request.

Initials MJ Initials EP

- The fee that the requester must pay to a private body is R50, provided that the requester may lodge and application to the court against the tender or payment of the request fee.
- After the Deputy Information Officer has decided on the request, the requester will be notified in the required form. If the request is granted, then a further access fee must be paid for reproduction and for search and preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure.
- The fee structure is available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za.

DigiCert has the right to reject any request for information submitted in terms of Sections 62 to 69 of the Act.

13. AVAILABILITY OF THE MANUAL

This PAIA Manual is made available as required by regulation, and is available for inspection at its listed premises in Section 2 as well as on its website at www.digicert.com.

Mike Johnson

Signature of Head of Private Body

Mike Johnson

Name of Head of Private Body

Aug 9, 2022

Date of Signature

Eric Porter

Signature of Head of Private Body

Eric Porter

Name of Head of Private Body

Aug 9, 2022

Date of Signature

Publication date of this manual: August 1, 2022

Next revision date of this manual: August 1, 2023

FORM C

REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Promotion of Access to Information Act, 2000
(Act No. 2 of 2000)

[Regulation 10]

A. Particulars of private body

The Head:

B. Particulars of person requesting access to the record

(a)	The particulars of the person who requests access to the record must be given below.
(b)	The address and/or fax number in the Republic to which the information is to be sent must be given.
(c)	Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:

Identity number:

Postal address:

Fax number:

Telephone number: E-mail address:

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed *ONLY if* a request *for information is* made on behalf of *another* person.

Full names and surname:

Identity number:

D. Particulars of record

(a)	Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
(b)	If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1 Description of record or relevant part of the record:

2 Reference number, if available:

3 Any further particulars of record:

E. Fees

(a)	A request for access to a record, other *than* a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b)	You will be *notified of* the amount required to be paid as the request fee.
(c)	The fee payable for access to a record depends *on* the form *in which* access is required and the reasonable time *required* to search for and prepare a record.
(d)	If you qualify for exemption *of* the payment *of* any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Disability:	Form in which record is required

Mark the appropriate box with an X.

NOTES:
(a) Compliance with your request in the specified form may depend on the form in which the record is available.
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
(c) The fee payable for access for the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:					
	copy of record*		inspection of record		
2. If record consists of visual images this includes photographs, slides, video recordings, computer-generated images, sketches, etc)					
	view the images		copy of the images"		transcription of the images*
3. If record consists of recorded words or information which can be reproduced in sound:					
	listen to the soundtrack audio cassette		transcription of soundtrack* written or printed document		
4. If record is held on computer or in an electronic or machine-readable form:					
	printed copy of record*		printed copy of information derived from the record"		copy in computer readable form* (stiffy or compact disc)

'If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO

G Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved/denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

Signed at…… This…… day of ……20

SIGNATURE OF REQUESTER / PERSON ON
WHOSE BEHALF REQUEST IS MADE